IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Dominquez et al.	Attorney Docket No.: VISAP073
Application No.: 10/660,263	Examiner: BAYAT, Bradley B.
Filed: September 10, 2003	Group: 3621
Title: DATA AUTHENTICATION AND PROVISIONING METHOD AND SYSTEM	Confirmation No.: 5063

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on April 14, 2008.

Signed: ______________/Laura M. Dean/_________________
Laura M. Dean

APPEAL BRIEF TRANSMITTAL
(37 CFR 192)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the Notice of Appeal filed in this case on February 14, 2008.

This application is on behalf of

□ Small Entity ☒ Large Entity

Pursuant to 37 CFR 1.17(f), the fee for filing the Appeal Brief is:
□ $255.00 (Small Entity) ☒ $510.00 (Large Entity)

□ Applicant(s) hereby petition for a _____ extension(s) of time to under 37 CFR 1.136.

If an additional extension of time is required, please consider this a petition therefor.

□ An extension for months has already been secured and the fee paid therefor of $ is deducted from the total fee due for the total months of extension now requested.

☒ Applicant(s) believe that no (additional) Extension of Time is required; however, if it is determined that such an extension is required, Applicant(s) hereby petition that such an extension be granted and authorize the Commissioner to charge the required fees for an Extension of Time under 37 CFR 1.136 to Deposit Account No. 50-4481.

Total Fee Due:

Appeal Brief fee	$510.00
Extension Fee (if any)	$
Total Fee Due	$510.00

□ Enclosed is Check No. in the amount of $.

☒ The Commissioner is authorized to charge the required fees, and/or any additional fees or credit any overpayment to Deposit Account No. 50-4481, (Order No. VISAP073).

Respectfully submitted,
BEYER LAW GROUP LLP

/ASH/
Alan S. Hodes
Reg. No. 38,185

P.O. Box 1687
Cupertino, CA 95015-1687
408-255-8001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex Parte Dominquez et al.

Application for Patent: 10/660,263

Filed: September 10, 2003

Group Art Unit: 3621

Examiner: BAYAT, Bradley B.

For: DATA AUTHENTICATION AND PROVISIONING METHOD AND SYSTEM

APPEAL BRIEF

BEYER LAW GROUP LLP
P.O. Box 1687
Cupertino, CA 95015-1687
Attorneys for Appellant

CERTIFICATE OF EFS-WEB TRANSMISSION
I hereby certify that this correspondence is being transmitted electronically through EFS-WEB to the Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on April 14, 2008.

Signed: ______________/Laura M. Dean/______________
Laura M. Dean

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

[37 CFR 41.37(c)(1)(i)]

The real party in interest is Visa International Service Association, a subsidiary of Visa Inc.

2. RELATED APPEALS AND INTERFERENCES

[37 CFR 41.37(c)(1)(ii)]

There are no related appeals. In at least one of the patent applications cross-referenced in the present patent application, one or more appeal briefs were filed. However, none of these appeals were allowed to reach the stage of being decided by the Board.

An interference was requested in patent application 10/384,735, which is in the same family as one of the patent applications cross-referenced in the present patent application. However, while the claims upon which the interference was requested remain pending, an interference has not been granted as of this time.

3. STATUS OF CLAIMS

[37 CFR 41.37(c)(1)(iii)]

The following claims have been rejected and appealed: claims 1-7, 9-18, 20-21, 23-37, 39-41, 44-47, 49-50 and 52-54.

The following claims have been cancelled: 8, 19, 22, 38, 42, 43, 48 and 51.

The claims on appeal are reproduced below in the Appendix at Section 9 of this Appeal Brief.

4. STATUS OF AMENDMENTS

[37 CFR 41.37(c)(1)(iv)]

No amendments were filed subsequent to final rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

[37 CFR 41.37(c)(1)(v)]

5.1. <u>Independent Claim 1</u>

Independent claim 1 is directed to a method (referring to Fig. 1) involving a presenter 708, a trusted party 710, and an acceptor 716 for validating submitted

profile data of said presenter during an on-line transaction. The method includes receiving, by the trusted party 710 during an enrollment process (Fig. 2), profile data (722, presenter file database) and enrollment data from said presenter, said trusted party being an issuer of an account to said presenter. Page 9, lines 6-20.
During the enrollment process, the trusted party verifies, using the data, the identity of said presenter and associates authentication data with the presenter. Page 9, lines 16-20.

The authentication data is communicated between the trusted party and the presenter during the enrollment process, the authentication data being known only to the trusted party and to the presenter. Page 8, lines 26-30.

Submitted profile data is received at the trusted party from the acceptor. Fig. 2, block 606; page 12, lines 13-17. The trusted party compares the submitted profile data against the profile data stored by the trusted party. Page 13, lines 26-29.

The trusted party receives submitted authentication data from the presenter during the on-line transaction. The trusted party authenticates the presenter by comparing the submitted authentication data received from said presenter with the authentication data already known by the trusted party. Page 12, line 30 to page 13, line 13.

The trusted party validates the submitted profile data using results of the comparing and results of the authenticating. The trusted party notifies the acceptor that the submitted profile data of the presenter is either authentic or erroneous, whereby said trusted party validates the submitted profile data of the presenter for the benefit of the acceptor. Fig. 2, 606; page 13, lines 19-26.

5.2. <u>Independent Claim 25</u>

Independent claim 25 is directed to an on-line data authentication system. A presenter 708 submits enrollment data and profile data to a trusted party 710 during an enrollment process (Fig. 2). Authentication data is associated with the presenter during the enrollment process (Page 9, lines 16-20). The authentication data is communicated between the presenter and the trusted party during the enrollment process. The authentication data is known only to the trusted party and to the presenter, the trusted party being an issuer of an account to the presenter. Page 8, lines 26-30.

The trusted party receives the enrollment data and the profile data during the enrollment process and verifies the identity of the presenter during the enrollment process using the enrollment data. Page 9, lines 16-20. The trusted party receives the authentication data from the presenter during an on-line transaction, and authenticates the authentication data and validates the profile data of the presenter during the on-line transaction. Page 12, line 30 to page 13, line 13.

An acceptor 716 conducts the on-line transaction with the presenter and requests of the trusted party to authenticate the presenter and to validate the profile data of the presenter. Fig. 2, 606; page 13, lines 19-26. A directory server 714 is configured to determine the existence of the trusted party and is able to authenticate the presenter and to validate the profile data of the presenter.

5.3. *Independent Claim 37*

Independent claim 37 is directed to a method involving a presenter 708, a trusted party 710, and an acceptor 716 for providing profile data of the presenter during an on-line transaction. The method includes receiving, by the trusted party during an enrollment process, profile data and enrollment data from the presenter, the trusted party being an issuer of an account to the presenter. Page 8, lines 26-30.

The method includes verifying, by the trusted party during the enrollment process using the enrollment data, the identity of the presenter and associating authentication data with the presenter. Page 9, lines 16-20.

The authentication data is communicated between the trusted party and the presenter during the enrollment process, the authentication data being known only to the trusted party and to the presenter. Page 8, lines 26-30.

The trusted party is queried by the acceptor for the trusted party to provide the profile data to the acceptor. Fig. 2, 608; page 12, lines 27-29. The trusted party receives submitted authentication data from the presenter during the on-line transaction. The trusted party compares the submitted authentication data against the authentication data previously associated with the presenter. Page 13, lines 1-13.

The profile data of the presenter is provided by the trusted party to the acceptor. The trusted party notifies the acceptor of the authenticity of the presenter, whereby the trusted party authenticates the presenter for the benefit of said acceptor and provides the profile data. Fig. 2, 608; page 12, lines 27-29.

5.4. Independent Claim 52

Independent claim 52 is directed to an on-line data authentication system. A presenter 708 submits enrollment data and profile data to a trusted party 710 during an enrollment process. Authentication data is associated with the presenter the enrollment process, and the authentication data is communicated between the presenter and the trusted party during the enrollment process The authentication data is known only to the trusted party and to the presenter, the trusted party being an issuer of an account to the presenter. Page 8, lines 26-30.

The trusted party receives the enrollment data and the profile data during the enrollment process, verifies the identity of the presenter during the enrollment process using the enrollment data, receives the authentication data from the presenter during an online transaction, and authenticates the authentication data and provides the profile data of the presenter to an acceptor during the on-line transaction. Page 13, lines 1-13; Fig. 2, 608; page 12, lines 27-29.

The acceptor conducts the on-line transaction with the presenter and requests the trusted party to authenticate the presenter and to provide the profile data of the presenter. Fig. 2, 606; page 13, lines 19-26. A directory server 714 is configured to determine the existence of said trusted party who is able to authenticate the presenter and to provide the profile data of the presenter.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

[37 CFR 41.37(c)(1)(vi)]

Ground I:

Claims 1-7, 9-18, 20, 21, 23-37, 39-41, 44-47, 49, 50 and 52-54 are rejected under 35 USC 103(a) as being unpatentable over Carrott (USP 6,839,692 B2) in view of Tsuei (US 2004/0083184 A1).

7. ARGUMENT

[37 CFR 41.37(c)(1)(vii)]

7.1. Ground I

7.1.1. *Claims 1-7, 9-18, 20, 21, 23-37, 39-41, 44-47, 49, 50 and 52-54*

It is respectfully submitted that the combination of Carrott and Tsuei does not yield the invention recited in claim 1. More particularly, the combination of Carrott and Tsuei does not include at least a disclosure or suggestion of verifying the identity of a presenter during an enrollment process.

Applicant appreciates the Examiner's detailed discussion in "Response to Arguments" (on page 2 of the final Office Action) paraphrasing Applicant's arguments that were considered by the Examiner. In particular, the Examiner notes "Applicant argues that the cited references fail to disclose any enrollment data used to identify the party (response p. 11). What Applicant actually argued, however, is (some emphasis added, some emphasis in original):

> In this present Reply E, Applicant would like to once again focus on a) – wherein **during an enrollment process**, a trusted party verifies the identity of the presenter using the enrollment data. The Examiner explicitly recognizes that Carrott, the primary reference, does not disclose a). ....We therefore look for any statement by the Examiner that Tsuei, the secondary reference, discloses a) – namely **an enrollment process** in which a trusted party verifies the identity of the presenter using the enrollment data.

The Examiner's "Response to Arguments," including citations to various portions of the Tsuei reference, make clear that the Examiner has apparently not considered the feature of Applicant's independent claims that a trusted party verifies the identity of a presenter "**during an enrollment process**."

The portions of Tsuei cited in the "Response to Arguments" section of the Office Action arguably disclose a registration process. However, any description of authentication in Tsuei is a description of "authentication" of a user's identify that takes place during a transaction, which is after the registration/enrollment process. The description of authentication in Tsuei is not a disclosure of verifying the identity of a user **during an enrollment process.**

For example, paragraph [0201] of Tsuei, which the Examiner cites in the "Response to Arguments" section of the Office Action, states in part that "the PMAC obtains customer name, billing information, mail delivery address, and possibly other information." There is also a statement in paragraph [0201] that "Once these data are collected and processed, the PMAC assigns a unique Private Mail Code to a customer." However, there is nothing to indicate that the processing referred to in this statement includes verifying the identity of the customer.

The Examiner also cites to paragraph [0202] of Tsuei in the Response to Arguments section of the Office Action. Paragraph [0202] discusses modifying subscription data. However, such modification is not during an enrollment process. Therefore, any "authentication process" in conjunction with such subscription data modification cannot be construed to be directed to verifying the identity of a presenter **during an enrollment process**. Furthermore, as has been discussed in previous responses, even if the presenter of the information was an imposter, as a result of the Tsuei enrollment/registration process, the imposter would be able to carry out transactions with respect to such information. In accordance with the subject matter recited in the independent claims, on the other hand, such information never would have made it into a central database since it would have been determined that the presenter of the information was an imposter during the process of attempting to verify the identity of the presenter.

Turing now to the body of the obviousness rejection, using Carrott and Tsuei, the Examiner notes (on page 5 of the Office Action):

> According to Tsuei, once a subscriber enrolls and registers providing profile and enrollment data, a unique identifier is associated with that customer, upon matching such data and verification of the identity and credentials of the customer, notification is provided for the benefit of the requesting party over the Internet......Therefore, it would have been obvious for one of ordinary skill in the art of the invention to modify Carrot's purchase transaction system to provide an anonymous transaction verification mechanism to provide security to the subscriber while at the same time providing further verification confirmation for the requester.

Further discussion of Tsuei by the Examiner (on page 6 of the Office Action) discusses assigning a password for use to authenticate the cardholder of an alias account.

From the assertions by the Examiner regarding Tsuei in the body of the obviousness rejection using Carrott and Tsuei, it is clear that the Examiner considers Tsuei for an alleged disclosure of authenticating a user during a transaction, and that the Examiner does **not** consider Tsuei at all to disclose verifying the identity of a presenter **during an enrollment process**, as required by claim 1.

In fact, as Applicant has discussed in past responses, and as Applicant has attempted to highlight above, nowhere does Tsuei disclose or suggest such a feature of verifying the identity of a presenter **during an enrollment process**.

For example, [0027] of Tsuei cited by the Examiner discloses:

> Preferably, the private facility administers the database, registers the customers, and assigns the mail codes to the registered customers before this anonymous mailing and relabeling service is started.

Nothing here discloses or suggests verifying the identity of a customer during the process of registering that customer.

A more detailed description of setting up a new account in the "alias account system" is set forth at [0090] et seq. of Tsuei. It is noted, for example, at [0091] that "The card applicant's real identity and factual information are provided on the part 1 credit card application 104." However, notably, there is no disclosure or suggestion that the "real identity" is in fact verified to be the identity of the customer during the enrollment process.

Furthermore, for example, [0170 et seq. of Tsuei discusses the "Account Acquisition Process." Here, it is discussed, for example, that "The issuer application processor 112 and the alias application processor 116 execute data entry step 1202." Additional steps include transmitting the data to the host processing system (HPS) and setting up the accounts based on the transmitted data. Notably, there is no disclosure or suggestion here, either, that the entered and transmitted data are verified to represent the true identity of the enrolling/registering customer during the enrollment process.

Tsuei, at [0201] describes activity related to a customer registering for a private mail service. There, it is disclosed that:

> During the registration process, see FIG. 27, the PMAC obtains customer name, billing information, mail delivery address, and possibly other information. Once these data are collected and processed, the PMAC assigns a unique Private Mail Code to a customer.

Again, though, there is no disclosure or suggestion that the PMAC or other functionality verifies the identity of the customer as part of the data collection/processing function of registering/enrolling the customer.

.

8. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner's rejection of claims 1-7, 9-18, 20-21, 23-37, 39-41, 44-47, 49-50 and 52-54 as being unpatentable is erroneous. Accordingly, the rejection should be reversed.

Respectfully submitted,
BEYER LAW GROUP LLP

/ASH/
Alan S. Hodes
Registration No. 38,185

BEYER LAW GROUP LLP
Attorneys for Appellant

9. CLAIMS APPENDIX
[37 CFR 41.37(c)(1)(viii)]

CLAIMS ON APPEAL

1. A method involving a presenter, a trusted party, and an acceptor for validating submitted profile data of said presenter during an on-line transaction, said method comprising:

receiving, by said trusted party during an enrollment process, profile data and enrollment data from said presenter, said trusted party being an issuer of an account to said presenter;

verifying, by said trusted party during said enrollment process using said enrollment data, the identity of said presenter and associating authentication data with said presenter;

communicating said authentication data between said trusted party and said presenter during said enrollment process, said authentication data being known only to said trusted party and to said presenter;

receiving said submitted profile data at said trusted party from said acceptor;

comparing said submitted profile data against said profile data stored by said trusted party;

receiving, at said trusted party, submitted authentication data from said presenter during said on-line transaction;

authenticating, by said trusted party, said presenter by comparing said submitted authentication data received from said presenter with said authentication data;

validating, by said trusted party, said submitted profile data using results of said comparing and results of said authenticating;

notifying said acceptor by said trusted party that said submitted profile data of said presenter is either authentic or erroneous, whereby said trusted party validates said submitted profile data of said presenter for the benefit of said acceptor.

2. A method as recited in claim 1 further comprising:

notifying said acceptor by said trusted party of the authenticity of said presenter, whereby said trusted party authenticates said presenter for the benefit of said acceptor.

3. A method as recited in claim 2 wherein said notifying operation further comprises:

notifying said acceptor that said presenter is authentic when said submitted authentication data received from said presenter matches said previously associated authentication data; and

notifying said acceptor that said submitted profile data is authentic when said submitted profile data matches said profile data.

4. A method as recited in claim 1 wherein the presenter communicates with said trusted party and with said acceptor over the Internet.

5. A method as recited in claim 4 wherein said trusted party and said acceptor also communicate over the Internet.

6. A method as recited in claim 3 wherein the notifying operation regarding the authenticity of said presenter provides a definitive answer as to whether the authenticity and the submitted profile data of said presenter are authentic or not.

7. A method as recited in claim 1 further comprising:

receiving and storing said authentication data from said presenter at said trusted party during said enrollment process, wherein said authentication data becomes associated with said presenter.

9. A method as recited in claim 1 further comprising:

providing, by said trusted party, to said presenter a program identity number which is correlated with said profile data and said authentication data; and

storing said program identity number by said trusted party.

10. A method as recited in claim 9 wherein said program identity number is an account number for a financial account of said presenter and wherein said trusted party is a financial institution that maintains said financial account.

11. A method as recited in claim 2, wherein prior to said trusted party receiving said authentication data, the method further comprising:

initiating communications between said presenter and said acceptor;

receiving said profile data~~,~~ and a program identity number at said acceptor from said presenter.

12. A method as recited in claim 11 further comprising:

querying said trusted party by said acceptor whether said presenter can be authenticated and whether said submitted profile data of said presenter can be validated by said trusted party.

13. A method as recited in claim 12 further comprising:

querying said trusted party by said acceptor whether account data updating can be provided.

14. A method as recited in claim 12 wherein the querying operation is executed by transmitting a service enrollment request message from said acceptor to said trusted party via a directory server.

15. A method as recited in claim 14 wherein said service enrollment request message includes said program identity number originally provided to said acceptor from said presenter.

16. A method as recited in claim 12 further comprising:

informing said acceptor by said trusted party whether said presenter can be authenticated and whether said profile data of said presenter can be validated by said trusted party.

17. A method as recited in claim 16 wherein the querying operation is executed by transmitting a service enrollment response message from said trusted party to said acceptor via a directory server.

18. A method as recited in claim 2 further comprising:

transmitting a data authentication request message from said acceptor to said trusted party in order to request that said trusted party authenticate said presenter and validate said submitted profile data of said presenter.

20. A method as recited in claim 18 wherein said data authentication request message includes submitted profile data originally provided to said acceptor from said presenter.

21. A method as recited in claim 18 wherein both of said notifying operations are executed by transmitting a data authentication response message from said trusted party to said acceptor.

23. A method as recited in claim 1 further comprising:

providing, by said trusted party, of updated profile data when said submitted profile data is determined to be out of date.

24. A method as recited in claim 23 wherein the updated profile data contains account data.

25. An on-line data authentication system comprising:

a presenter who submits enrollment data and profile data to a trusted party during an enrollment process, and with whom is associated authentication data during said enrollment process, wherein said authentication data is communicated between said presenter and said trusted party during said enrollment process, said authentication data being known only to said trusted party and to said presenter, said trusted party being an issuer of an account to said presenter;

said trusted party who receives said enrollment data and said profile data during said enrollment process, who verifies the identity of said presenter during said enrollment process using said enrollment data, who receives said authentication data from said presenter during an on-line transaction, and who authenticates said authentication data and validates said profile data of said presenter during said on-line transaction;

an acceptor who conducts said on-line transaction with said presenter and who requests of said trusted party to authenticate said presenter and to validate said profile data of said presenter; and

a directory server configured to determine the existence of said trusted party who is able to authenticate said presenter and to validate said profile data of said presenter.

26. A system as recited in claim 25 wherein each of said acceptor and said trusted party are configured to communicate with said presenter via the Internet.

27. A system as recited in claim 25 wherein the trusted party is configured to provide a definitive answer as to whether said presenter and said profile data are authentic or not authentic.

28. A system as recited in claim 25 further comprising:

pre-designated authentication data previously submitted by said presenter, which is stored by said trusted party, wherein said trusted party authenticates said authentication data by comparing said authentication data against said pre-designated authentication data.

29. A system as recited in claim 28 further comprising:

a program identity number that is assigned to said presenter wherein said program identity number is correlated to said pre-designated authentication data and said profile data.

30. A system as recited in claim 29 wherein said program identity number is an account number for a financial account of said presenter wherein said trusted party is a financial institution that maintains said financial account.

31. A system as recited in claim 25 further comprising:

a service enrollment request message that is transmitted from said acceptor to said trusted party via said directory server, said service enrollment request message containing a query to said directory server and trusted party as to whether said trusted party will be able to authenticate said presenter and validate said profile data of said presenter.

32. A system as recited in claim 31 further comprising:

a service enrollment response message that is transmitted from said trusted party to said acceptor via said directory server, said service enrollment response message containing confirmation as to whether said trusted party will be able to authenticate said presenter and validate said profile data of said presenter.

33. A system as recited in claim 25 further comprising:

a data authentication request message that is transmitted from said acceptor to said trusted party in order to request that said trusted party authenticate said presenter and validate said profile data of said presenter.

34. A system as recited in claim 33 wherein said data authentication request message includes said profile data of said presenter.

35. A system as recited in claim 33 further comprising:

a data authentication response message that is transmitted from said trusted party to said acceptor, said data authentication response message including notification as to the authenticity of said presenter and the validity of said profile data of said presenter.

36. A system as recited in claim 33 further comprising:

a data authentication response message that is transmitted from said trusted party to said acceptor, said data authentication response message including notification as to whether said profile data is accurate or contains errors.

37. A method involving a presenter, a trusted party, and an acceptor for providing profile data of said presenter during an on-line transaction, said method comprising:

receiving, by said trusted party during an enrollment process, profile data and enrollment data from said presenter, said trusted party being an issuer of an account to said presenter;

verifying, by said trusted party during said enrollment process using said enrollment data, the identity of said presenter and associating authentication data with said presenter;

communicating said authentication data between said trusted party and said presenter during said enrollment process, said authentication data being known only to said trusted party and to said presenter;

querying said trusted party by said acceptor for said trusted party to provide said profile data to said acceptor;

receiving, at said trusted party, submitted authentication data from said presenter during said on-line transaction;

comparing, by said trusted party, said submitted authentication data against said authentication data previously associated with said presenter;

providing said profile data of said presenter, by said trusted party, to said acceptor; and

notifying said acceptor by said trusted party of the authenticity of said presenter, whereby said trusted party authenticates said presenter for the benefit of said acceptor and provides said profile data.

39. A method as recited in claim 37 wherein the presenter communicates with said trusted party and with said acceptor over the Internet.

40. A method as recited in claim 39 wherein said trusted party and said acceptor also communicate over the Internet.

41. A method as recited in claim 37 wherein the notifying operation regarding the authenticity of said presenter provides a definitive answer as to whether the authenticity and said profile data of said presenter are authentic or not.

44. A method as recited in claim with claim 37 further comprising:

providing, by said trusted party, to said presenter a program identity number which is correlated with said profile data and with said authentication data;

storing said program identity number by said trusted party.

45. A method as recited in claim 44 wherein said program identity number is an account number for a financial account of said presenter wherein said trusted party is a financial institution that maintains said financial account.

46. A method as recited in claim 37 wherein said profile data includes at least the name and address of said presenter.

47. A method as recited in claim 37 further comprising:

transmitting a data authentication request message from said acceptor to said trusted party in order to request that said trusted party provide said profile data of said presenter.

49. A method as recited in claim 37 further comprising:

requesting said presenter, by said trusted party, for said authentication data; and

asking said presenter, by said trusted party, for permission to provide said profile data of said presenter to said acceptor.

50. A method as recited in claim 47 wherein said providing is executed by transmitting a data authentication response message from said trusted party to said acceptor, said data authentication response message containing said profile data of said presenter.

52. An on-line data authentication system comprising:

a presenter who submits enrollment data and profile data to a trusted party during an enrollment process, and with whom is associated authentication data during said enrollment process, wherein said authentication data is communicated between said presenter and said trusted party during said enrollment process, said authentication data being known only to said trusted party and to said presenter, said trusted party being an issuer of an account to said presenter;

said trusted party who receives said enrollment data and said profile data during said enrollment process, who verifies the identity of said presenter during said enrollment process using said enrollment data, who receives said authentication data from said presenter during an online transaction, and who authenticates said authentication data and provides said profile data of said ~~a~~ presenter to an acceptor during said on-line transaction;

said acceptor who conducts said on-line transaction with said presenter and who requests of said trusted party to authenticate said presenter and to provide said profile data of said presenter; and

a directory server configured to determine the existence of said trusted party who is able to authenticate said presenter and to provide said profile data of said presenter.

53. A system as recited in claim 52 wherein each of said acceptor and said trusted party are configured to communicate with said presenter via the Internet.

54. A system as recited in claim 52 wherein the trusted party is configured to provide a definitive answer as to whether said presenter is authentic or not authentic.

10. EVIDENCE APPENDIX

[37 CFR 41.37(c)(1)(ix)]

No evidence has been submitted pursuant to §§ 1.130, 1.131, or 1.132 of 37 CFR, nor has any other evidence been entered by the examiner.

11. RELATED PROCEEDINGS APPENDIX
[37 CFR 41.37(c)(1)(x)]

There have been no decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 CFR 41.37(c)(1).